UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/775,617	02/05/2001	Kaoru Uchida	Q62922	8357

7590 11/02/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/775,617	UCHIDA, KAORU	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 05 February 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

2. The disclosure is objected to because of the following informalities:

- On page 12, line 7, "describe" should be –described–.
- On page 25, line 22m "attach" should be –attack–.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-11 and 13-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Glass et al. (U.S. Patent No. 6,332,193).

Regarding claims 1 and 24, Glass et al. teaches a system comprising:

- A biometric data input device (fig. 2, ref. num 4); and
- A biometric verifier connected to the biometric data input device (fig. 2, ref. num 10),

Wherein the biometric data input device comprises:

- A biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data (fig. 2, ref. num 6 and 8); and
- An encoder for encoding the digital biometric data using secret information to transmit encoded data to the biometric verifier (col. 2, line 58 through col. 3, line 1), and

The biometric verifier comprises:

- A decoder for decoding the encoded data using the secret information to reproduce digital biometric data (col. 7, lines 3-15);
- A verifier for verifying identity of the individual based on the digital biometric data (fig. 2, "Matcher").

Regarding claim 2, Glass et al. teaches wherein the secret information is a unique key identifying the biometric data input device (col. 6, lines 10-18).

Regarding claims 3 and 25, Glass et al. teaches wherein the verifier comprises:

- A feature extractor for extracting a feature of the digital biometric data decoded by the decoder (col. 7, lines 34-40);

- A first determiner for determining whether the feature of the digital biometric data is a registered biometric feature of an authorized user, by comparing the feature of the digital biometric data against previously registered biometric features (col. 7, lines 40-44);
- A second determiner for determining whether the biometric data input device is an authorized device, based on the secret information (col. 6, lines 18-32); and
- A third determiner for determining that the individual is an authorized user when the feature of the digital biometric data is a registered biometric feature of an authorized user and the biometric data input device is an authorized device (col. 9, lines 26-59).

Regarding claims 4, 13, 21, and 26, Glass et al. teaches a system comprising:

- At least one biometric data input device (fig. 2, ref. num 4); and
- A biometric verifier connected to the at least one biometric data input device (fig. 2, ref. num 10),

Wherein each of the at least one biometric data input device comprises:

- A biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data (fig. 2, ref. num 6 and 8); and
- An encrypter for encrypting the digital biometric data using an encryption key to transmit encrypted data to the biometric verifier, wherein the encryption key identifies the biometric data input device (col. 10, lines 59-65), and

The biometric verifier comprises:

- A table storing an encryption key corresponding to each of said at least one biometric data input device (col. 5, lines 32-34);
- A decrypter for decrypting the encrypted data using the encryption key corresponding to the biometric data input device to reproduce digital biometric data (col. 10, lines 65-66);
- A comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a comparison result (fig. 2, "Biometric Template Store"); and
- A determiner for determining whether the individual is an authorized person, based on the comparison result and correctness of the digital biometric data decrypted by the decrypter (fig. 2, "Matcher").

Regarding claims 5 and 27, Glass et al. teaches wherein the determiner determines the correctness of the digital biometric data decrypted by the decrypter depending on whether a type of the digital biometric data decrypted by the decrypter matches that of the digital biometric data outputted by the biometric data input device (col. 9, lines 26-59).

Regarding claims 6, 8, 10, 15, 18, and 20, Glass et al. teaches wherein a fingerprint is used as the physical characteristic (col. 1, lines 34-37).

Regarding claims 7, 16, 22, and 28, Glass et al. teaches a system comprising:

- At least one biometric data input device (fig. 2, ref. num 4); and
- A biometric verifier connected to the at least one biometric data input device (fig. 2, ref. num 10),

Wherein each of the at least one biometric data input device comprises:

- A biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data (fig. 2, ref. num 6 and 8);
- A watermark encoder for embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data (fig. 5);
- An encrypter for encrypting the watermarked biometric data to produce encrypted data (col. 10, lines 59-65); and
- A transmitter for transmitting the encrypted data and a device identification identifying the biometric data input device to the biometric verifier (col. 9, lines 37-40), and

The biometric verifier comprises:

- A table storing secret information corresponding to a device identification for each of said at least one biometric data input device (col. 5, lines 32-34);
- A decrypter for decrypting the encrypted data to produce watermarked digital biometric data (col. 10, lines 65-66);
- A watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data decrypted by the decrypter (col. 7, lines 12-33);

- A first comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result (fig. 2, "Biometric Template Store");
- A second comparator for comparing the watermark data separated by the watermark decoder with secret information corresponding to the device identification identifying the biometric data input device to produce a secret information comparison result (col. 7, lines 24-33); and
- A determiner for determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result (fig. 2, "Matcher").

Regarding claims 9, 19, 23, and 29, Person teaches a system comprising:

- At least one biometric data input device (fig. 2, ref. num 4); and
- A biometric verifier connected to the at least one biometric data input device (fig. 2, ref. num 10),

Wherein each of the at least one biometric data input device comprises:

- A biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data (fig. 2, ref. num 6 and 8);
- A watermark encoder for embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data (fig. 5);
- A first encrypter for encrypting the watermarked biometric data to produce encrypted biometric data (col. 10, lines 59-65);

- A second encrypter for encrypting the secret information using a public key of asymmetric encryption scheme to produce encrypted secret information (col. 6, lines 25-28); and
- A transmitter for transmitting the encrypted biometric data and the encrypted secret information (col. 9, lines 37-40), and

The biometric verifier comprises:

- A first decrypter for decrypting the encrypted biometric data to produce watermarked digital biometric data (col. 10, lines 65-66);
- A second decrypter for decrypting the encrypted secret information to produce received secret information (col. 6, lines 25-28);
- A watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data decrypted by the decrypter (col. 7, lines 12-33);
- A first comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result (fig. 2, "Biometric Template Store");
- A second comparator for comparing the watermark data separated by the watermark decoder with the received secret information to produce a secret information comparison result (col. 7, lines 24-33); and
- A determiner for determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result (fig. 2, "Matcher").

Regarding claim 11, Glass et al. teaches wherein the biometric verifier is connected to the at least one biometric data input device via a network (fig. 2, ref. num 9).

Regarding claims 14 and 17, Glass et al. teaches the biometric data sensor, the memory, and the encrypter are inseparably implemented in one piece (fig. 3).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Glass et al. (U.S. Patent No. 6,332,193) in view of Li et al. (U.S. Patent No. 6,219,793).

Regarding claim 12, Glass et al. teaches all the limitations of claims 9 and 11, above. However, Glass et al. does not teach wherein the encrypted biometric data and the encrypted secret information are transmitted to the biometric verifier through different channels.

Li et al. teaches wherein the encrypted biometric data and the encrypted secret information are transmitted to the biometric verifier through different channels (col. 1, lines 45-49).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to transmit the two separate data through different channels, as taught by Li et al., with the system of Glass et al. It would have been obvious for such modifications because one channel can be secure while the other remains insecure, thus allowing the secret information to be transmitted without a usurper discovering the key.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100